Statement of Need

1. **Title of Project:**

   Pagers and Pager Services

2. **Description:**

   The intent of this contract is for one vendor to supply the James A Haley Veterans Hospital (JAHVH) with digital numeric and alpha numeric pagers for use both in-house and wide area paging, as well as offer a pager management package.

3. **Scope of Need:**

   - Vendor shall employ all measures necessary to ensure a short response time, including modifications to network transmitters.
   - Vendor service shall provide group paging on both alpha and numeric pagers.
   - Vendor shall provide within their offer the guaranteed response time, as well as the average response time.
   - Statewide coverage is required for all non-emergency medical response pagers.
   - Pager Service shall be for an unlimited number of pages.
   - If this solicitation results in a new Contractor providing the pager services, the new Vendor shall not charge the VA for the first month of service during the transition from current Vendor to new Vendor.

   Digital tone pagers:

   - Approximately 1400 digital tone pagers are currently required under this contract.
   - Digital tone pagers shall have a numeric display.
   - Digital tone pagers shall include belt clips and battery covers.
   - Response time for digital tone pagers shall not exceed 60 seconds when paged via direct dial phone number or by use of Vendor's web site.

   Alpha Numeric Pagers:

   - Approximately 153 alpha-numeric pagers are currently required under this contract.
   - Alpha numeric pagers shall include belt clips and battery covers.

- Response time for alpha Numeric pagers shall not exceed 60 seconds when paged via direct dial phone number or by use of Vendor's web site.

Two Way Pagers:

- 2-way paging which can provide for message delivery and read receipts

Emergency Medical Response pagers:

- Approximately 140 of the 153 alpha-numeric pagers are currently used for emergency medical response within the main facility; therefore it is imperative that the paging system provide as short a response time as possible.

- Response time for emergency code pagers shall not exceed 10 seconds when the paging system is directly access via paging terminal and shall not exceed 45 seconds by use of Vendor's web site

- Transmission for the emergency medical response pagers shall be on a dedicated medical frequency.

- Currently the JAHVA has direct access via paging terminal to the current Vendor's paging system for activation of emergency medical response group pages. The paging terminal is software based application installed on each of the four (4) JAHVH Operators computer work station. This is a mandatory requirement and the Vendor shall incur any and all costs associated with the direct access to their system. Example would be a lease line from the telephone company to connect our location and the Vendor location.

- Vendor shall provide the JAHVA with a number of spare pagers of each type. Spare pagers will be for used as immediate replacement of non functioning pagers and for growth. Spare pagers will not incur monthly recurring charges until they are activated. Number of spares to be agreed upon by Vendor and JAHVA after award of contract but shall be at a minimum 10% of the number of active pagers.

Maintenance Support

- Provide 24x7x365 telephone support for troubles.

- Provide 24x7x365 process to escalate trouble calls to the next level of support.

Customer Service:

- Provide Customer support via telephone.

- Provide Customer support thru an internet web portal.

Vendor System Outages

- Vendor shall immediately notify the Contracting Officer's Technical Representative (COTR) or other authorized persons when the paging system and/or associated equipment become inoperable. This shall include an emergency notification system.

- The Contractor shall provide the COTR with updates every 30 minutes until the system becomes operable.

- At no time shall service be unavailable in excess of 6 hours.

- The Contractor shall establish Emergency Operating Procedures which includes but not limited to the following (a copy of said plan will be provided with the offer):
    - System outage notification
    - Partial service notification plan
    - System outage response procedures
    - Severe weather response procedures
    - Satellite failure contingency plan

Coverage Area:

- Service shall include any necessary transmitter(s) to provide 100% reception through the James A. Haley Veterans' Hospital.

- Any necessary boosters (receivers) shall be installed via coordination thru the Contracting Officer and COTR.

- Contractor shall provide numeric paging service which penetrates all parts of the following buildings:
    - James A. Haley Veterans' Hospital campus (Tampa, FL)
    - University of South Florida campus (Tampa, FL)
    - Shiner's Hospital campus (Tampa, FL)
    - Moffitt Cancer Center campus (Tampa, FL)
    - Tampa General Hospital (Tampa, FL)
    - All Children's Hospital (St. Petersburg, FL)
    - Bay Pines VAMC (St. Petersburg, FL)

- Prior to any contract award the Vendor shall provide sampling and testing of the pagers and equipment they offer to insure that coverage and response times are met.

- The Vendor shall contact the COTR, Jessica Trevena, via email @ jessica.trevena@va.gov or (813) 903-2494 to schedule testing of their offered system and pagers. The backup shall be Ann Morales, ann.morales@va.gov or (813) 245-2410.

- The COTR will direct and accompany all Vendors to the same areas in the facility for testing.

Pager Management Program:

- A management program shall have the capability of:
  - Creating and managing on-call schedules.
  - Allow forwarding of pages to another device.
  - Reports that includes but not limited to device logs, delivery receipts, and read receipts.
  - Allow administrators of the system to activate, deactivate, and swap pager numbers from one device to another device.
  - A plan shall be developed and submitted for the installation and training of this program.
  - Training shall be for OI&T Technical Staff, System Administrator and End User.

4. Performance Period:

01/01/2012-09/30/2012

Option Year 1 10/01/2012 – 09/30/2013
Option Year 2 10/01/2013 – 09/30/2014
Option Year 3 10/01/2014 – 09/30/2015
Option Year 4 10/01/2015 – 09/30/2016

5. Type of Contract:

Firm Fixed

"The Certification and Accreditation (C&A) requirements do not apply and a Security Accreditation Package is not required for this SON. "

Security Impact is LOW per HB 6500.

VA ACQUISITION REGULATION SOLICITATION PROVISION AND CONTRACT CLAUSE

NOTE: This clause will undergo official rule making by the Office of Acquisitions and Logistics. The below language will be submitted for public review through the *Federal Register*. The final wording of the clause may be changed from what is outlined below based on public review and comment. Once approved, the final language in the clause can be obtained from the Office of Acquisitions and Logistics Programs and Policy.

1. SUBPART 839.2 – INFORMATION AND INFORMATION TECHNOLOGY SECURITY REQUIREMENTS

839.201 Contract clause for Information and Information Technology Security:

a. Due to the threat of data breach, compromise or loss of information that resides on either VA-owned or contractor-owned systems, and to comply with Federal laws and regulations, VA has developed an Information and Information Technology Security clause to be used when VA sensitive information is accessed, used, stored, generated, transmitted, or exchanged by and between VA and a contractor, subcontractor or a third party in any format (e.g., paper, microfiche, electronic or magnetic portable media).

b. In solicitations and contracts where VA Sensitive Information or Information Technology will be accessed or utilized, the CO shall insert the clause found at 852.273-75, Security Requirements for Unclassified Information Technology Resources.

2. 852.273-75 - SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (INTERIM- OCTOBER 2008)

As prescribed in 839.201, insert the following clause:

The contractor, their personnel, and their subcontractors shall be subject to the Federal laws, regulations, standards, and VA Directives and Handbooks regarding information and information system security as delineated in this contract.

(END OF CLAUSE)

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE FOR INCLUSION INTO CONTRACTS, AS APPROPRIATE

1. GENERAL

Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

a. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COTR, and approved by the VA Privacy Service in accordance with Directive 6507, *VA Privacy Impact Assessment*.

b. The contractor/subcontractor shall certify to the COTR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

c. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default "program files" directory and silently install and uninstall.

d. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

e. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

f. The contractor/subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.
g. The contractor/subcontractor agrees to:

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

(a) The Systems of Records (SOR); and

(b) The design, development, or operation work that the contractor/subcontractor is to perform;

(1) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

(2) Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

h. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the contractor/subcontractor is considered to be an employee of the agency.

(1) "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

(2) "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.
(3) "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

6. SECURITY INCIDENT INVESTIGATION

a. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COTR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.

b. To the extent known by the contractor/subcontractor, the contractor/subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

7. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the contractor/subcontractor processes or maintains under this contract.

b. The contractor/subcontractor shall provide notice to VA of a "security incident" as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-

Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

(1) Nature of the event (loss, theft, unauthorized access);

(2) Description of the event, including:

(a) date of occurrence;
(b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code; (3) Number of individuals affected or potentially affected;
(4) Names of individuals or groups affected or potentially affected;

(5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
(6) Amount of time the data has been out of VA control;
(7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

(8) Known misuses of data containing sensitive personal information, if any;
(9) Assessment of the potential harm to the affected individuals;
(10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
(11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the contractor shall be responsible for paying to the VA liquidated damages in the amount of $__37.50___ per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

(1) Notification;

(2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
(3) Data breach analysis;
(4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
(5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

(6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

8. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the government, the contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

9. TRAINING

a. All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

(1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix E relating to access to VA information and information systems;

(2) Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;
(3) Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
(4) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

b. The contractor shall provide to the contracting officer and/or the COTR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.